Overview of the MERMOS Human Reliability Analysis method

11th August 2010, Idaho Falls

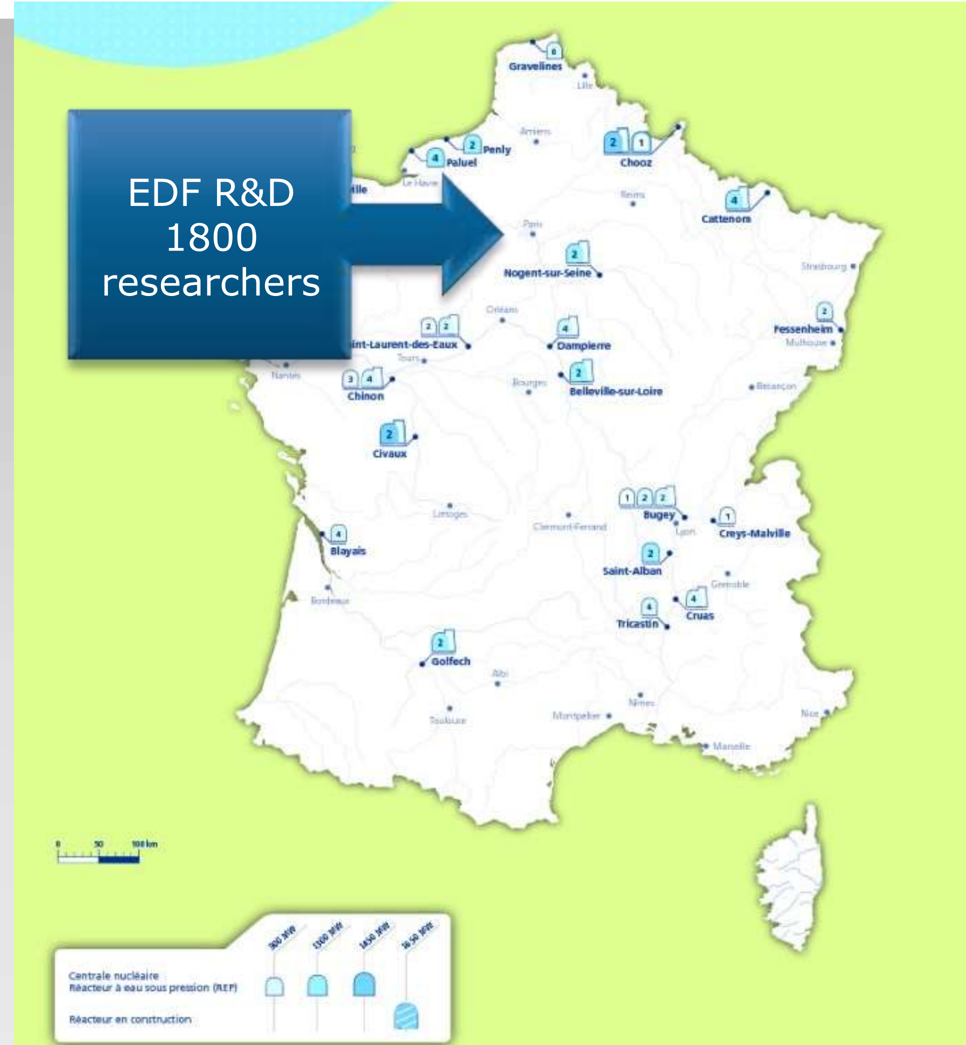
Pierre LE BOT

- Introduction
- Why do accidents occur because of humans ?
- Key concepts
- MERMOS process
- Important issues
- Let’s analyse

Introduction

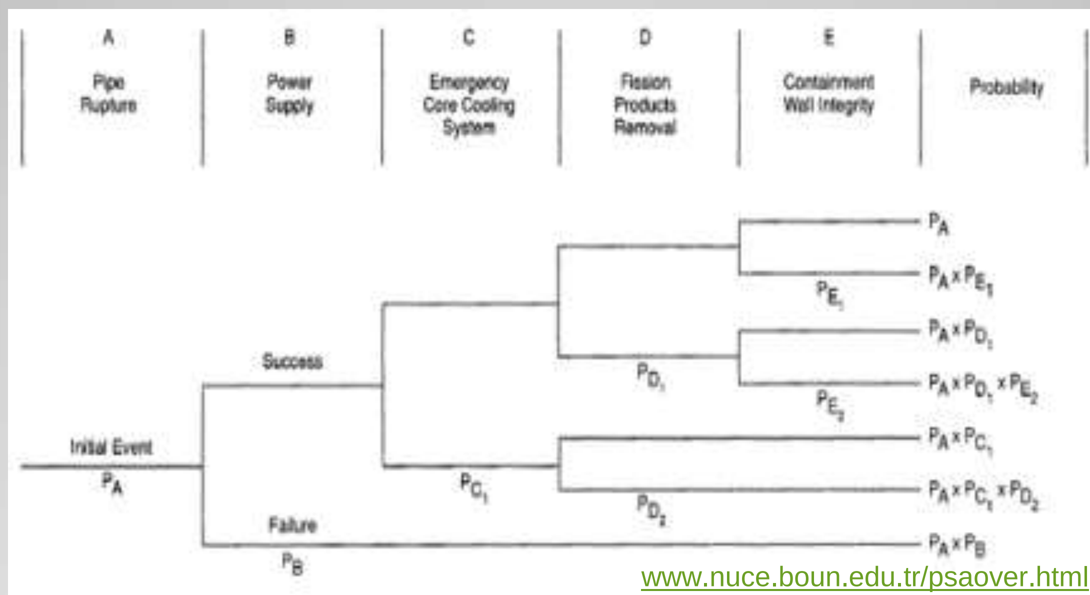
Nuclear operator

- installed capacity: 128,200 GW
- 156.500 employees in the world
- In France 58 nuclear units at 19 plants – all PWR (4 main series)
- 1100 reactors.years cumulated experience
- High level of standardization within a series

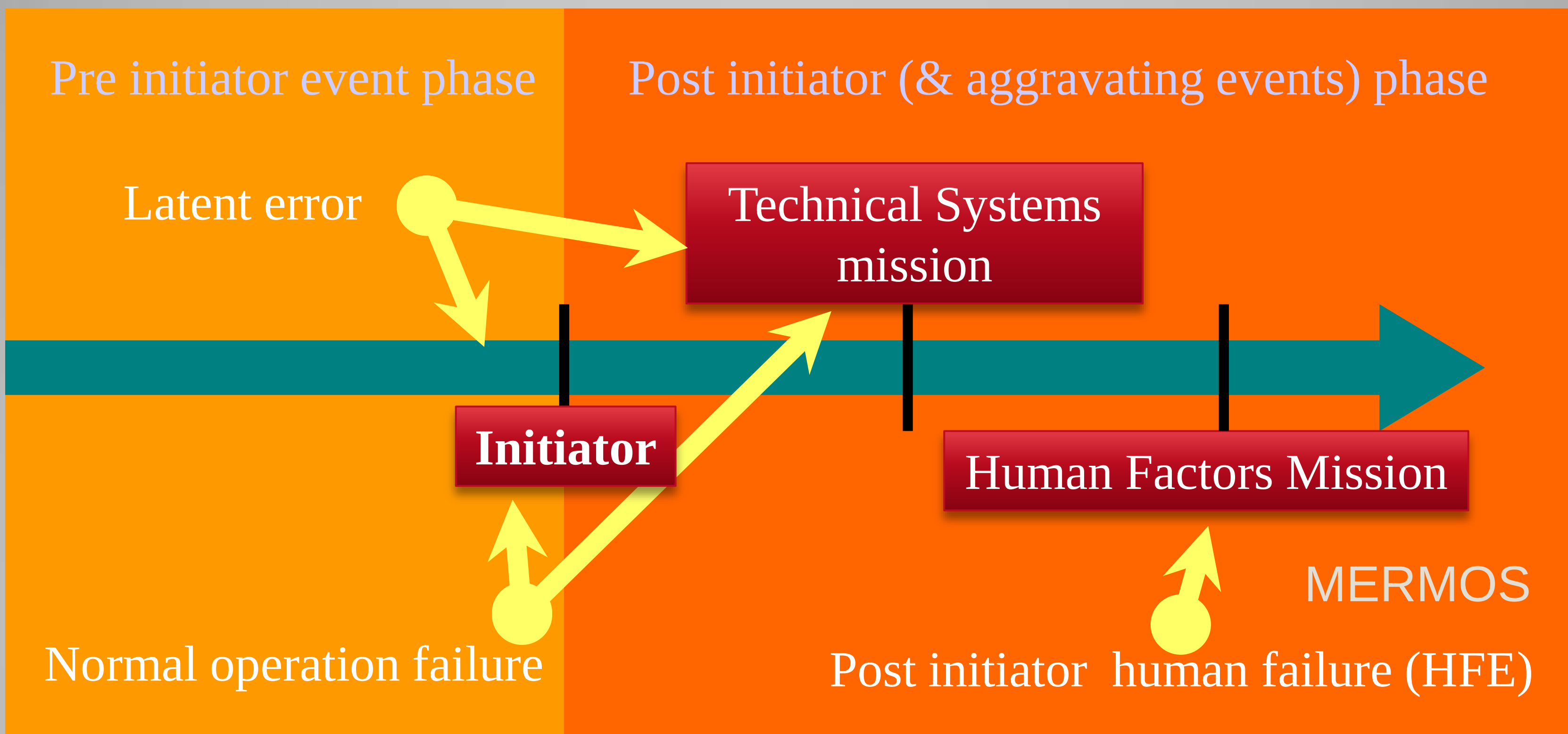


EDF’s PSA reference models

- Five PSA (Probabilistic Safety Assessment) level 1+
  (impact of sequences: core damage)
- 1 full level 2 model
  (impact of sequences: radioactive releases due to core damage)
- Generic data for one series or for the whole fleet
- Reference methods



HRA for NPP's PSA



Normal operation
Maintenance

Emergency operation

MERMOS origin

"Méthode d'Evaluation de la Réalisation des Missions Opérateurs pour la Sûreté"
Method for assessing the completion of operators action for safety

First EDF's PSAs HRA for classic control room & paper procedures

- Adaptation of THERP and ASEP
- Extensive use of data from simulator

N4 series with full computerized interface and procedures

- First methods based on deviation from procedures not applicable
- Extensive feedback (simulators observations and ergonomists studies)

➔ MERMOS

Why do accidents occur because of humans ?

Ultra safe systems: Humans role in safety ?

Human can't be perfect and can err

Automatize or h

Improve interfa
procedures, trai ig

Require procedures strict application

Engineering can't be perfect nor predict everything

anage safety by

culture, skills, experience

Require situation awareness & initiatives

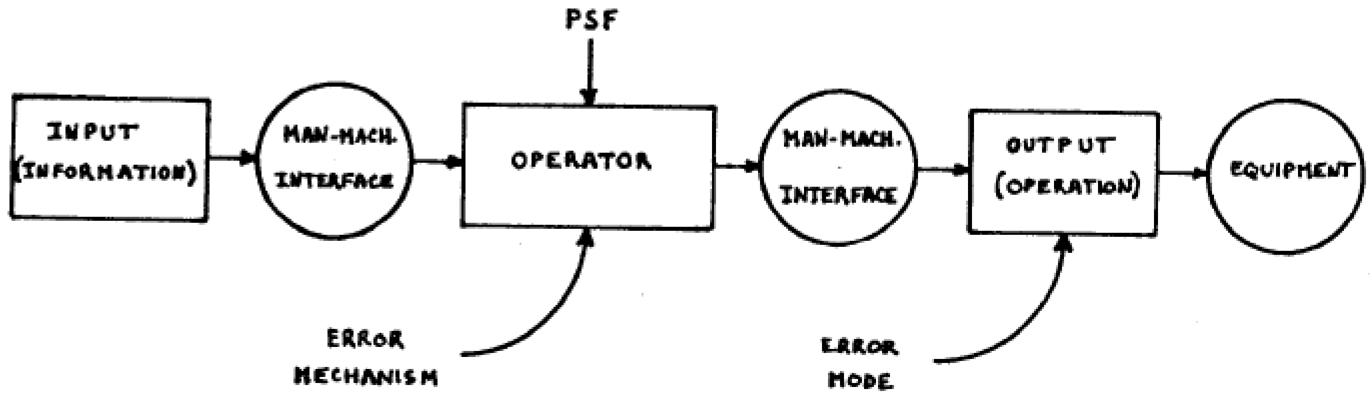
Anticipation

Adaptation

First HRA models

OLD VISION : unrationally, operator sometimes does'nt perform expected action

- Operator = machine
  - Without autonomy
  - With limited capacities
  - Very unreliable
- Human failure:
  - Individual
  - Operator informed and sollicitated by interface and procedure
  - If response is not as expected➔ **Error**



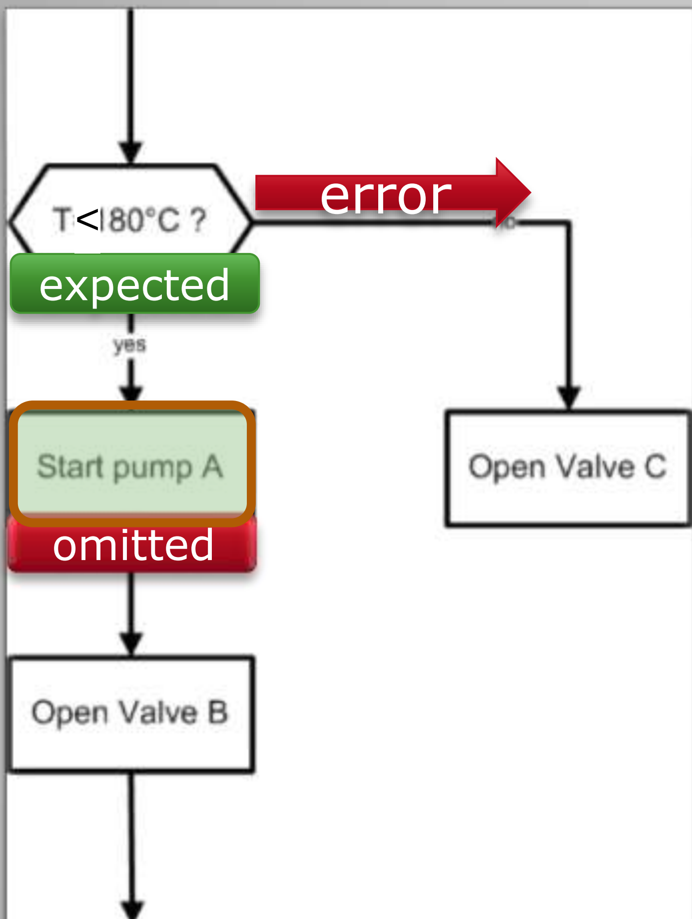
THE BASIS OF THE ERROR DESCRIPTION FORM : AN ELEMENTARY MODEL OF HUMAN BEHAVIOR

FIGURE 1

A. Villemeur, F. Mosneron-Dupin, M. Bouissou, T. Meslin *"A Human Factors Databank For French Nuclear Powerplants", Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems, American Nuclear Society, Knoxville, TN.(1986)*

First Human Reliability paradigm at EDF (1986)

How to identify and assess potential Human Failure Event ? An engineering problem for HRA



- The classical engineer approach (1rst generation method):
  - Failure = the omission of the expected actions prescribed in the applicable procedure

  ➔Screening of the prescribed actions, depending on their consequences

  - **HFE of EOO (error of omission)** are easy to identify
  - No clear method for **EOC (error of commission)** or limited
    - Not easy to find out plausible potential unexpected output
    - No clear validation from operational feedback

- Have you understood what happens ?
- Did they do errors ?
  - The supervisor believed that the generator failed to start
  - They deviate from the prescribed operation: direct application of the procedure PR01 (treatment of the loss of the electric power source)
- Is it an omission ? A commission error ?

Our conclusion is that the classic HRA model has to be improved.

We needed new paradigm and concepts.

Issues

KEY CONCEPTS

The Emergency Operating System (EOS)
The CICAs
The scenarios of failure
The SAD functions

EDF R&D

The Emergency Operating System

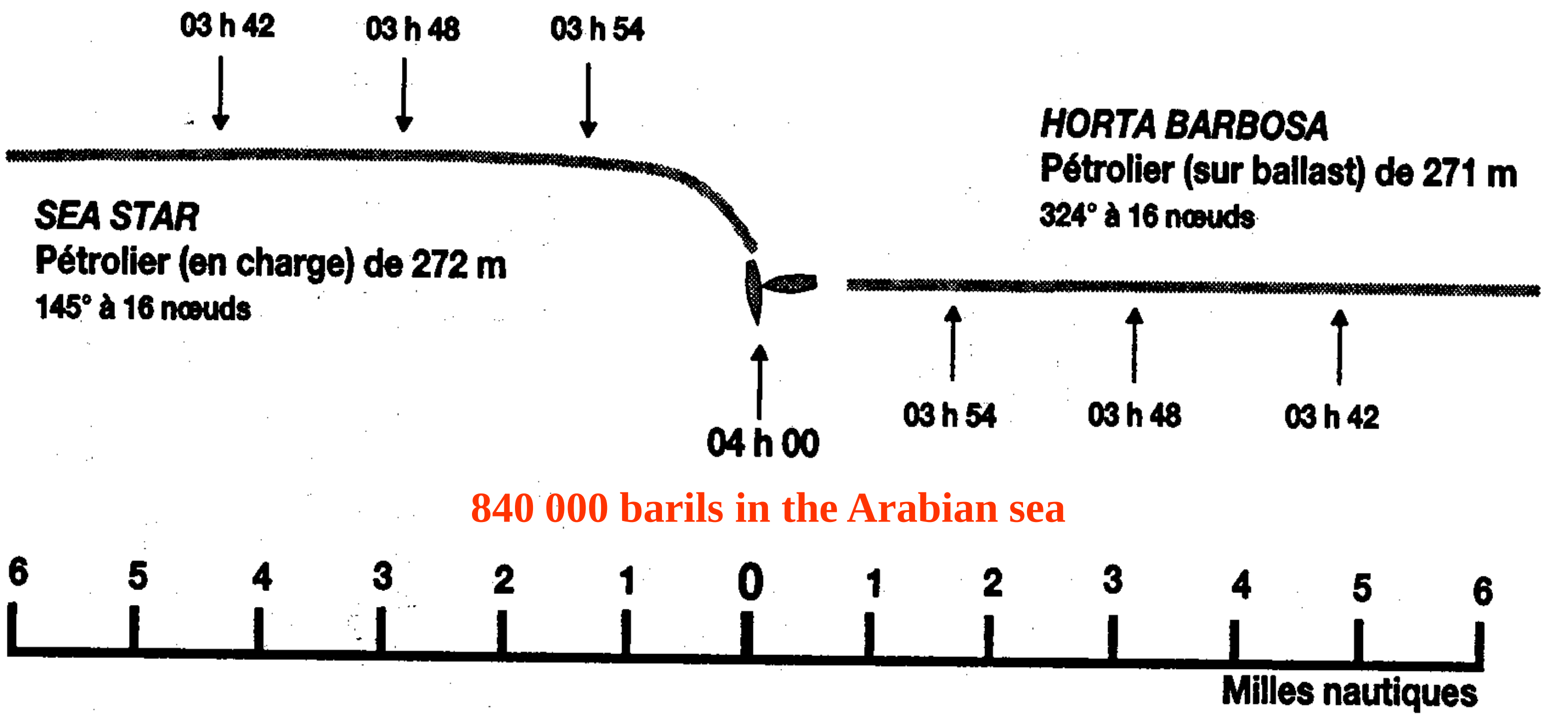
- Emergency operation of a NPP is **emerging from interaction between operators, procedures and interface** that constitute a system (EOS)
- The EOS is **cognitive and distributed**
  - It uses prior knowledge and produces new knowledge in real time
  - Knowledge is deposited in and elaborated by different system components.

Human reliability is the reliability of the EOS

The CICAs

Figure 2

Collision entre le *Sea Star* et le *Horta Barbosa*,
le 19 décembre 1972



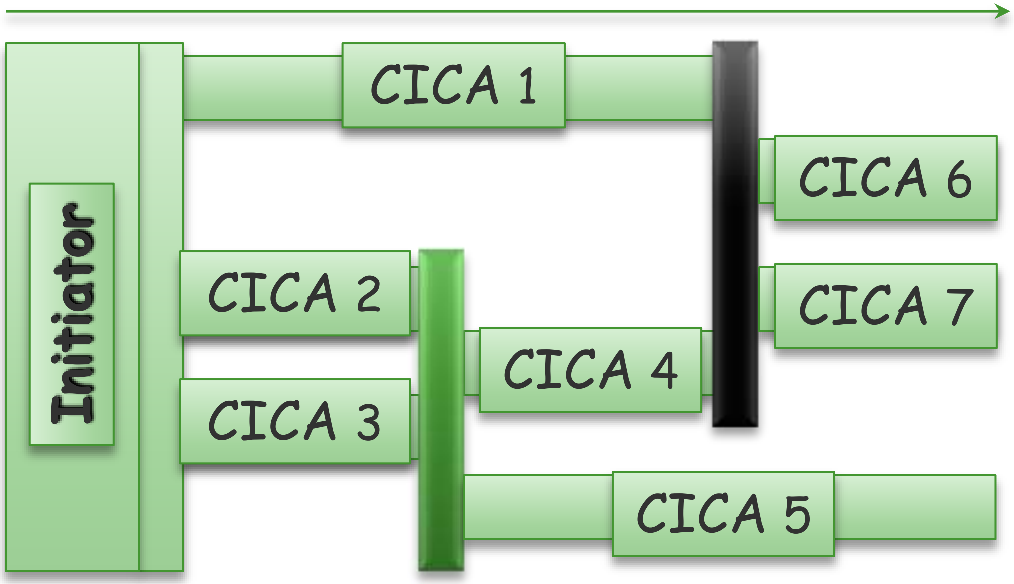
Dessin de l'auteur d'après *Le Grand Atlas de la mer*, Paris, Encyclopaedia Universalis, p. 215.

J. Morel

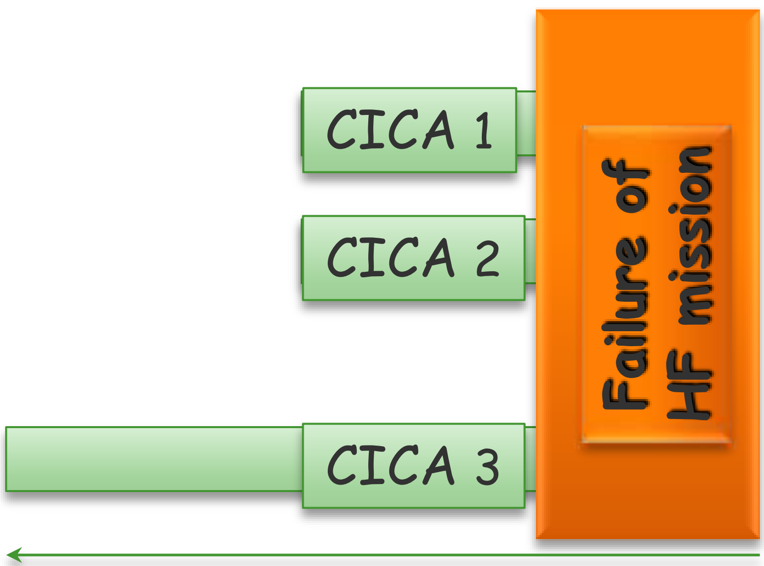
- A CICA is **a collective rule** that:
  - the EOS has decided (explicitely or not) to follow in a **stable phase**
  - determines its **configuration and orientation in time**
  - is stopped by a **rupture phase** and a **reconfiguration** as soon as it is detected that the objective is reached or the CICA is no more fitted to the situation
- Exemple: TMI

04:00	**rupture1**	**from normal to emergency operation**
04:03	**stability 1**	**management of excessive SI + recovery of AFS**
04:16	**rupture 2**	**reconfiguration towards stabilization**
04:20	**stability 2**	**stabilization + local investigations**
05:13	**rupture3**	***system disorientation***
05:42		***core is uncovered***

Definition and example



Retrospective analysis

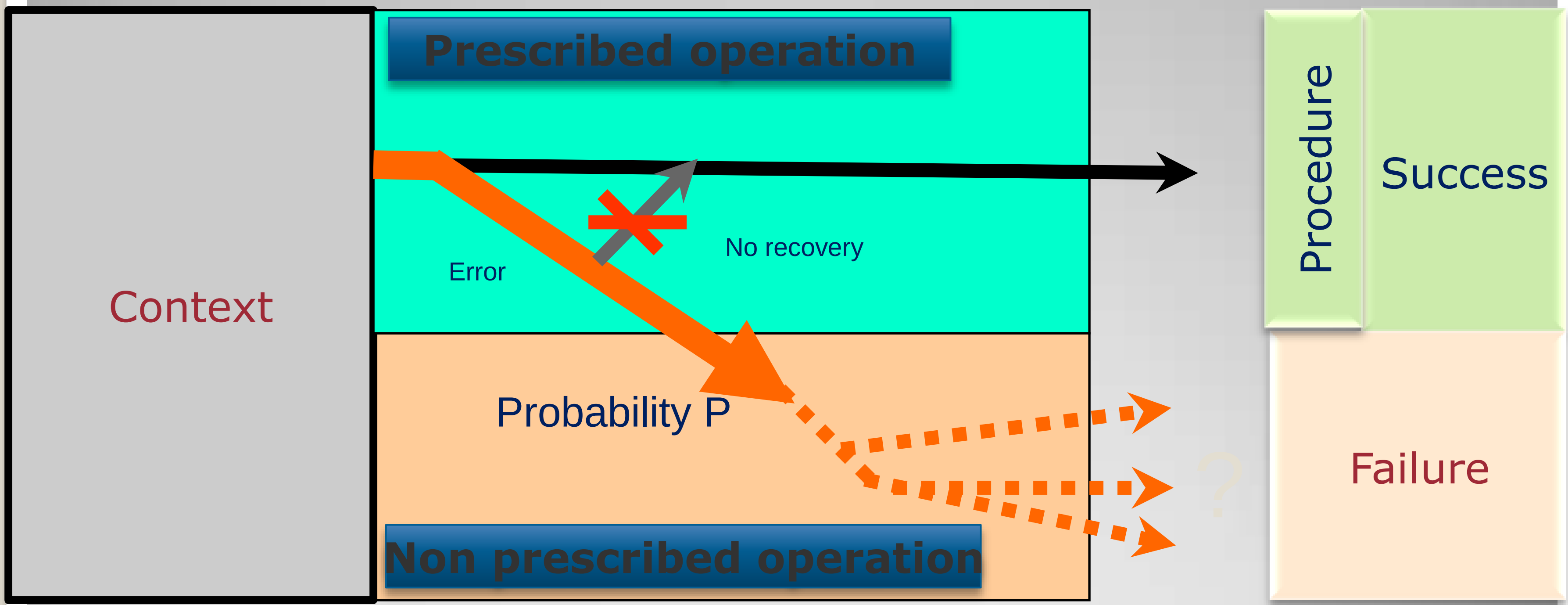


Human Reliability Analysis

The scenarios of failure

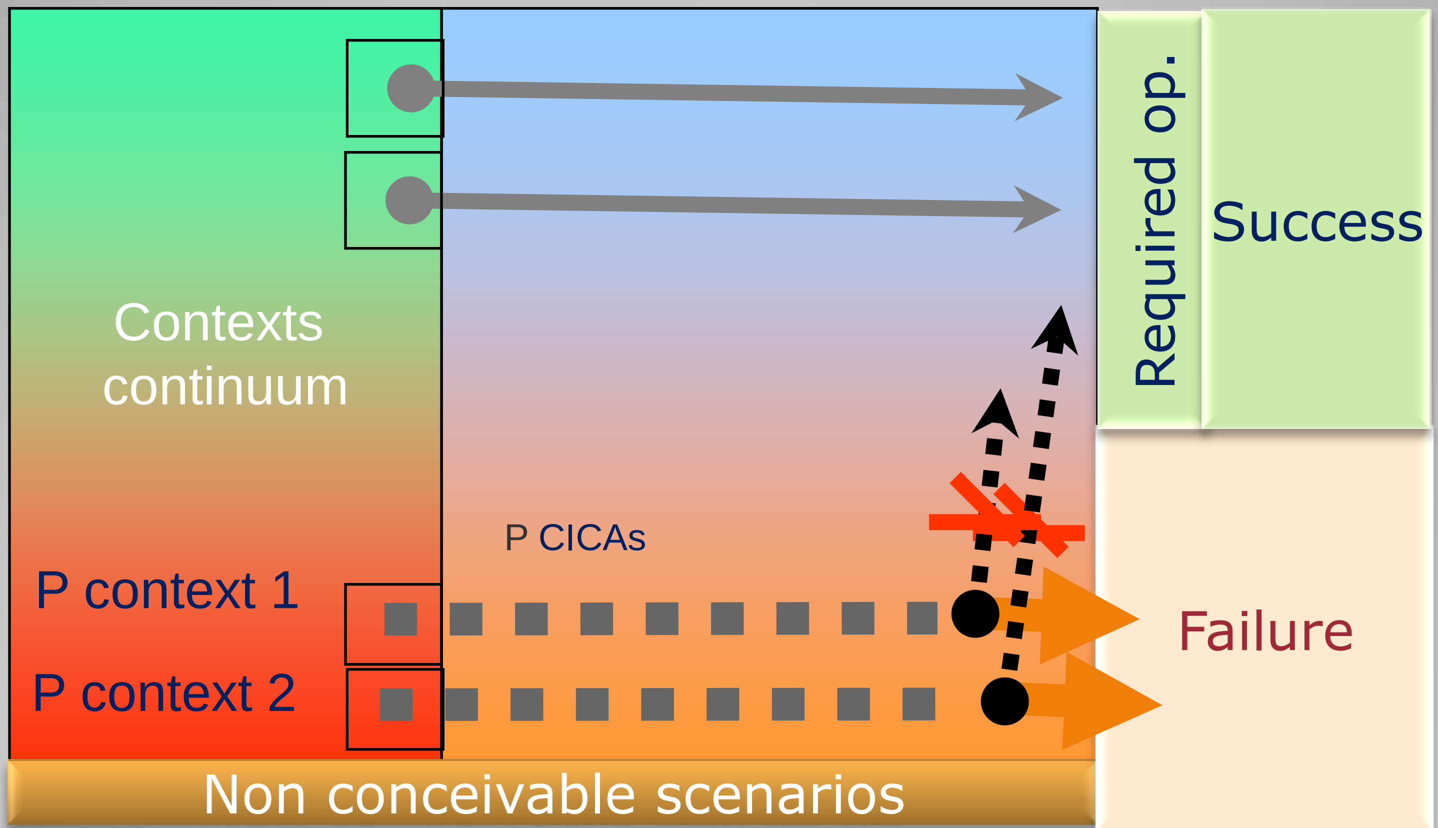
Former models based on error and deviation from expected operation
MERMOS failure model: the scenarios of failure

Former models based on error and deviation from expected operation



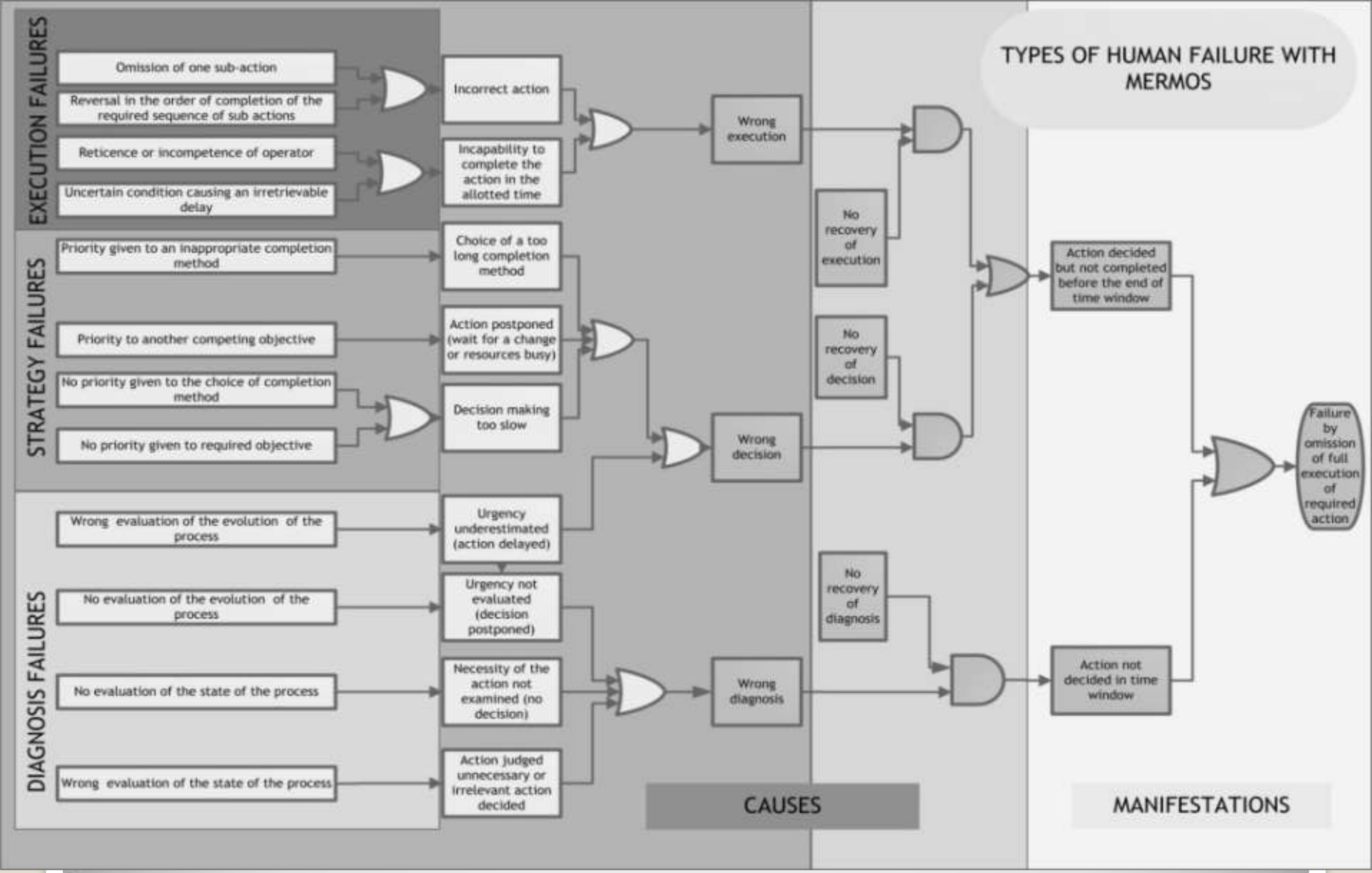
UNLIKELY ERRONEOUS OPERATION IN ONE UNIC LIKELY CONTEXT

MERMOS failure model: the scenarios of failure



LIKELY COHERENT OPERATIONS IN RARE CONTEXTS

« PARTIR DE L'ECHEC »



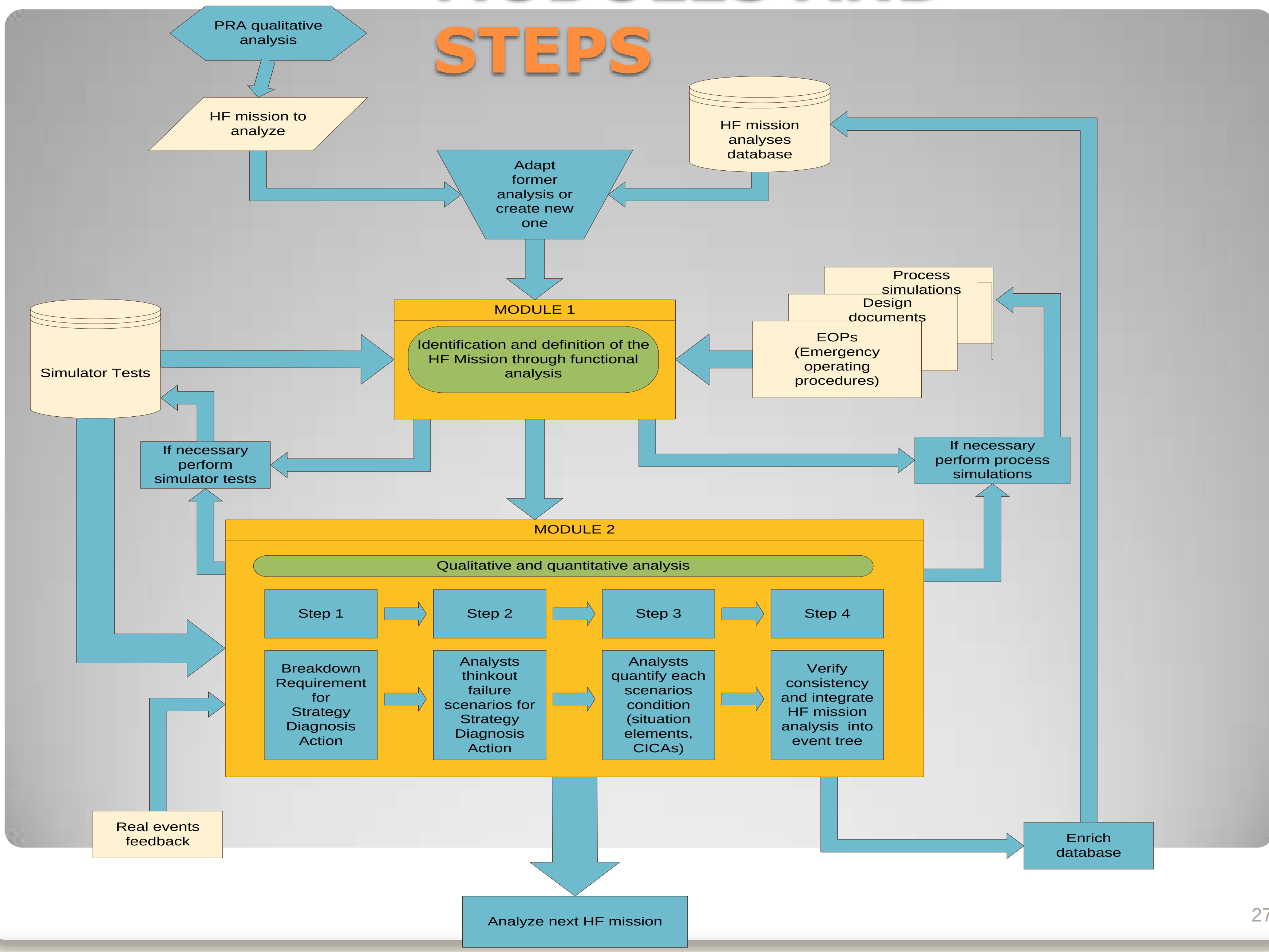
SAD Functions: strategy, action, diagnostic (state/situation)

MERMOS process

- To build (and upgrade) the answer to the question :
  - How could the Emergency Operation System fail ?
  - In rare situations and in a plausible way
  - By describing operational stories leading to failure (= MERMOS scenarios)

Goal of the analyst

MODULES AND STEPS



Structure of MERMOS analysis / quantification

$$P(HFE\ failure) = P_{residual} + \sum_{i=1\ to\ n} P(scenario\ i)$$

Steamline Break + SGTR, auto-isolation of the break (complex scenario)

Cooldown the RCS within 15 minutes from E-3 step 7

Probability of mission failure (HEP):	1.0 E-2
Uncertainty:	3.7 E-4 to 3.7 E-2

N°	Scenarios	Prob.
1	The system hesitates about the means and does not operate the cooldown early enough	8.1 E-3
2	Before operating the cooldown, the system wants to make sure that the SG has been well locally isolated	7.3 E-4
3	The system tries first to reach ruptured SG level > 17% narrow range, and starts the cooling too late	0
4	The team does not choose the expeditious cooldown given a reading error of the level of the SG	8.1 E-5
5	the system interrupts too early the cooling given a reading error on a parameter that governs the stopping of the cooling, and does not restarts on time	2.4 E-4
6	the system is cooling too much and overtakes the limit of subcooling margin	9 E-5
7	the system operates an unsufficient cooling because of an error of rating and of lack of communication	8.1 E-4
Pr	-	6 E-5

Example

$$P(scenario\ i) = P(context) \times P(operation)_{/context} \times P(non\ reconfiguration)$$

Context (or situation)	• Conjonction of situation features • Given the initiating and aggravating events
Operation (given the context)	• Configuration and orientation of the EOS (coherent and justified) • CICAS
Non reconfiguration	• Wrong operation is lasting too long

Scenario structure /quantification

Example of MERMOS scenario

SCENARIO n°1	Probability: 8.1 E-3
Description : **The system hesitates about the means and does not operate the cooldown early enough**	

Situation feature	
The operators hesitate on the means to use before operating the cooldown	0.1
The supervisor asks for a meeting to decide which means is to be used.	0.3

CICA	
Suspension of the following of the procedure	0.9

No reconfiguration probability :	0.3

Stage1	• **Breakdown of requirements with SAD functions**
Stage 2	• **Qualitative Analysis : design of scenarios**
Stage 3	• Verifications
Stage 4	• **Quantification by experts judgments and statistics**
Stage 5	• Adjustments

Steps of Module 2

QUANTIFICATION

- STATISTICS
- (3) EXPERTS JUDGMENTS
  1. Quantification of each element of each scenario by each expert
  2. Comparison
  3. New quantification
  4. Vote

Scale (not obligatory)

(Sure)	**(1)**
Very probable	0.9
Quite probable	0.3
Not very probable	0.1
Very unprobable	0.01
Impossible	0

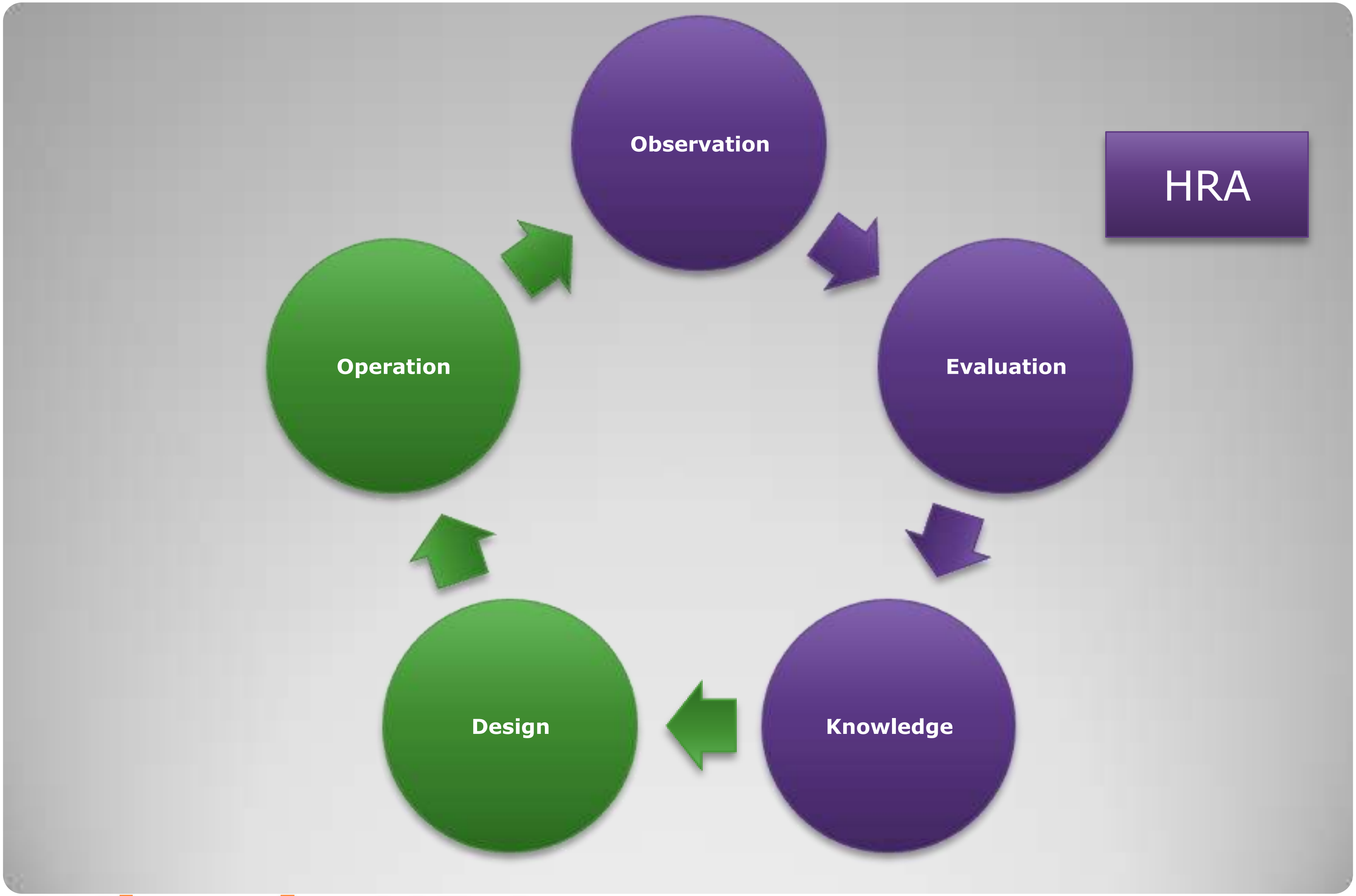
Important issues

Human error
What is HRA

Human error

- Not the point to focuse on
- Taxonomy of errors : not very useful
- Commission / omission errors (EOC/EOO)

Macro level : (functional)	EOO : Omission of required activation of a safety function
Meso level : (emergency operating system)	EOC : Intentional and coherent operation that causes an EOO at the upper level
Micro level : (individual)	EOO or EOC (influences the context that leads to the EOC at the upper level)



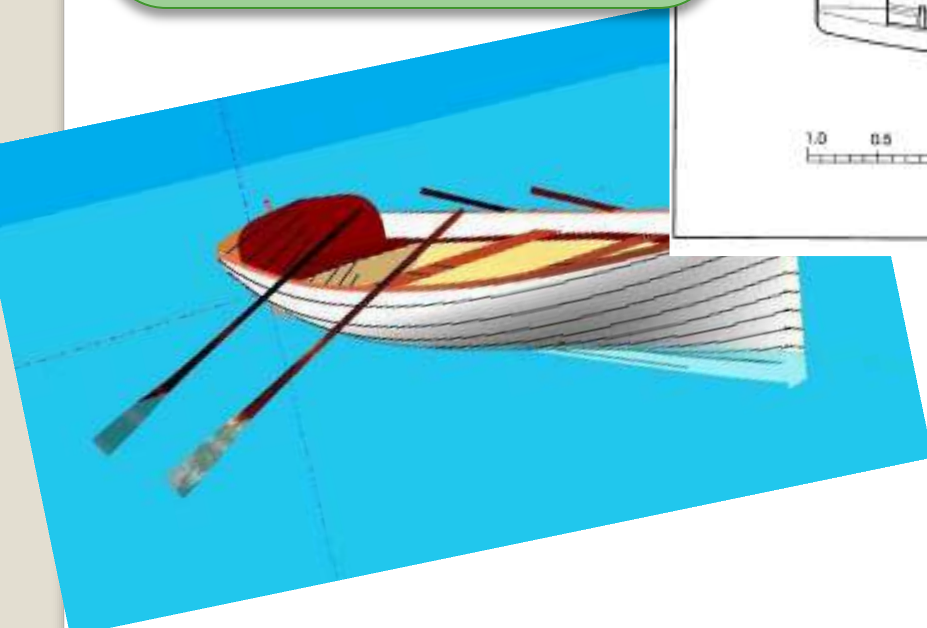
What is HRA

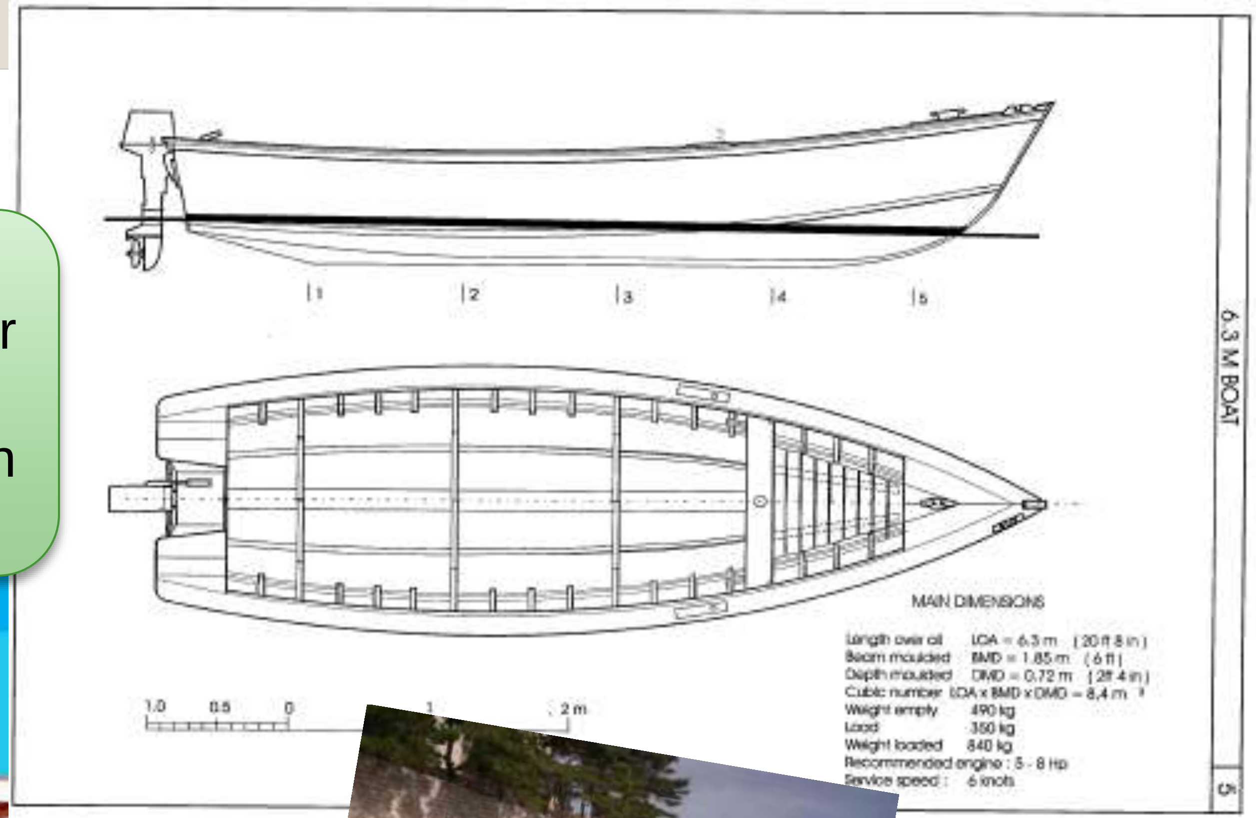
Let’s analyse

Little Titanic

Picture of the ship

1/3 sailors are experimented in motor mechanics
½ are experimented in navigation





Fishing boat (*FAO fisheries technical paper, Oyvind Gulbrandsen, Norway, Food and agriculture organization of the United Nations, Rome, 2004*)

Example : Little Titanic
(risk of sinking of a fishing boat)

- System : Fishing boat with a motor, a pump for water and a net, anchored off the coast, and two fishermen with two oars to row.
- Initiating event : loss of a drainage-hole plug (1/2 inch hole in the hull of the boat), not reparable nor compensable, + the hold pump does not work + the engine will not start (not repairable) ; (...)
- Mission : to get back to the port before the boat sinks (within 60 minutes), first hauling in the net, then rowing to the coast (with one rower, or two if any delay)

- The crew may attempt to restart the engine at all costs and not reach the coast in time
- The crew may take too much time hauling in the net and not reach the coast in time
- …

First ideas of failure scenarios ?

- 1/ The crew, who are sleeping, do not assess the situation *(no state diagnosis)*
- 2/ The crew do not diagnose the unavailability of the engine early enough to save themselves *(erroneous diagnosis of state)*
- 3/ The crew, hoping for the arrival of a lifeboat, stay where they are too long and do not row fast enough *(erroneous diagnosis of situation : incorrect estimation of the kinetics)*

Failure scenarios found with MERMOS

- 4/ The crew persevere in attempting to repair the engine and do not get back to the coast in time *(erroneous diagnosis of situation: they do not realise that their attempts will completely fail)*
- 5/ The crew, slowed down by the weather, use a single rower *(erroneous strategy)*
- 6/ The crew take too long hauling in the net *(erroneous action, meaning action not performed effectively)*

MERMOS scenarios (2/3)

- 7/ Following a problem, the net remains stuck to the boat and slows its progress *(erroneous action: the crew does not abandon the net)*
- 8/ The crew makes a navigational error, takes the wrong course and maintains it due to poor visibility *(erroneous action: following the wrong course).*

MERMOS scenarios (3/3)

SCENARIO INL/NRC	Probability: 1.8E-3
Description : **The EOS overestimates leak rate—row too quickly and get tired**	

Situation features	
Mismatched experience with leaks (different hull design, small rain adding water) leads to overestimation	0.25
Fear of drowning.	0.2
Unable to row quickly and make it to shore (limited endurance)	0.1

CICA	
Get to shore as fast as possible	0.9

No reconfiguration probability:	0.4

A new scenario by trainees

Next part: the Model of Resilience in Situation

pierre.le-bot@edf.fr

SAD Function :	***Failure mode :***
Strategy	No strategy

Element of requirements not satisfied :
Give priority to isolation of the ruptured SG, to avoid its filling

Non satisfaction modality:

SCENARIO n°1	**Probability:** [redacted]

Situation features	**Proba**	**Justification**

N°	**CICA**	**Proba**	**Justification**

No reconfiguration probability :	
Justification:	

SAD Function :	***Failure mode :***
Strategy	No strategy
Element of requirements not satisfied : Give priority to isolation of the ruptured SG, to avoid its filling	
Non satisfaction modality: Absence of priority and acceleration of operation in the event of delay	

SCENARIO n°1	**Probability:** [redacted]
Description : The system does not perform the procedural steps fast enough and does not reach the step of the isolation of the ruptured SG within the allotted time.	

Situation features	Proba	Justification
- The operators shut down the reactor late		
The operators follow the instructions cautiously		
- The SS does not incite the operators to accelerate the procedural path		

N°	CICA	Proba	Justification
1	- Run through the procedures step by step		

No reconfiguration probability :	
Justification:	